Microsoft Azure

Cloud Governance & Compliance

Syed Safdar Hussain

(Cloud Solutions Architect)

02-March-2023

veraqor

unveiling data. unleashing potential

Agenda

CAF & Why Governance

Defining Your Initial Governance State

Governance Methodology Overview

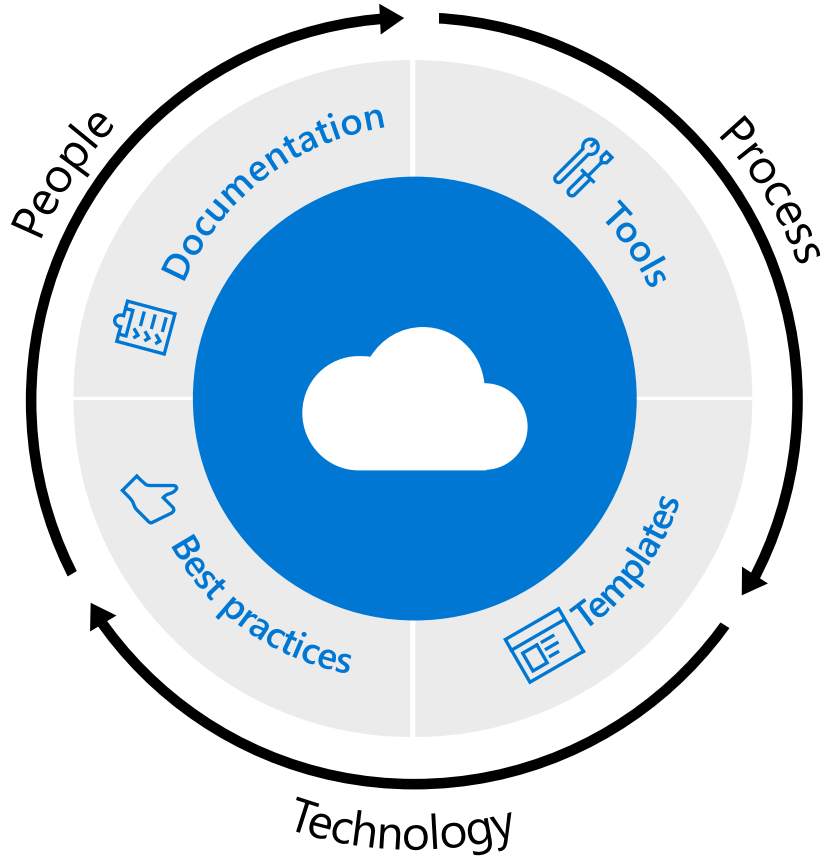
Take Action

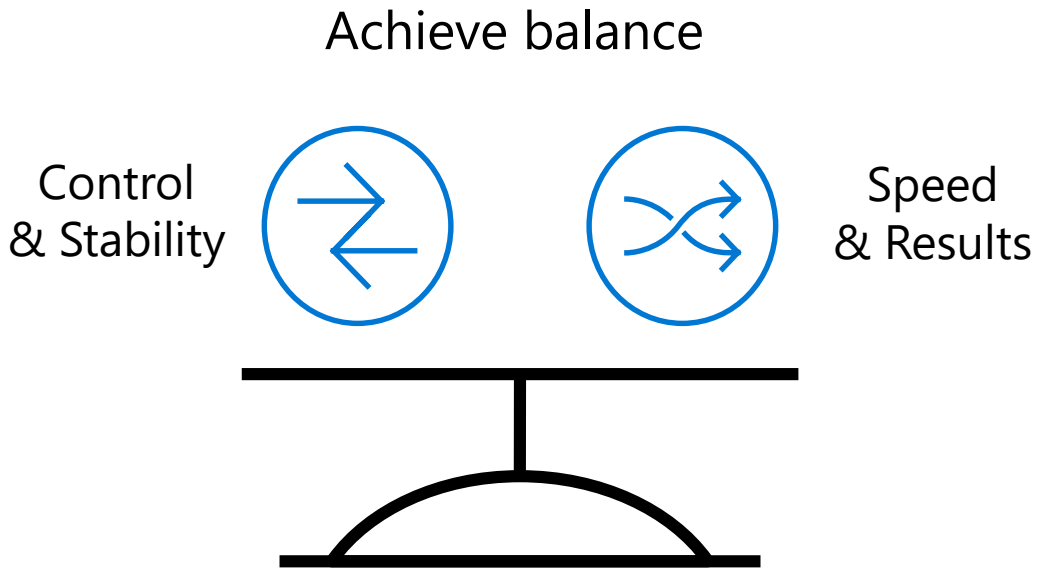
Governance as Actionable Model

Veraqor Offers

veraqor

Microsoft Cloud Adoption Framework for Azure



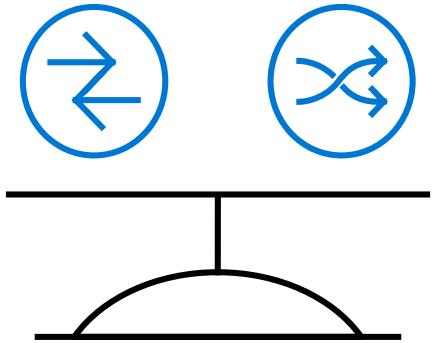


Align business, people and technology strategy.
Achieve business goals with actionable, efficient, and comprehensive guidance.
Deliver fast results with control and stability.

veraqor

Why is Governance Important?

Transformation



Risk mitigation

- Maintaining full compliance
- Creating better cost visibility and control
- Improving security posture
- Being agile—to support scale

Who is responsible for monitoring? support? And operations?

Which services should be migrated to Azure?

What roles & responsibilities must be defined?

What security measures should I consider?

What are the core processes needed for service management?

How do I ensure a balance between innovation, cost and agility?

What organizational changes are needed?

What key capabilities I must develop?

Azure governance building blocks?

Microsoft Azure

Governance Methodology Overview

veraqor
unveiling data. unleashing potential

Drive cloud adoption efficiency in an iterative governance process – four key exercises to focus on:

1. **Methodology overview**
   Establish a basic understanding of cloud governance

2. **Governance benchmark**
   Assess your current state and the future state to get started

3. **Initial governance foundation**
   Begin establishing your governance foundation by implementing a set of governance tools

4. **Evolve governance foundation**
   Iteratively add governance controls to address risks

Governance Methodology

Envision an end state – and incrementally build trust and confidence.

Govern

Define corporate policy

Business risks

Document evolving business risks and the business' tolerance for risk, based on data classification and application criticality

Policy & compliance

Convert risk decisions into policy statements to establish cloud adoption boundaries

Process

Establish processes to monitor violations and adherence to corporate policies.

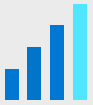
Five disciplines of cloud governance

Cost management

Evaluate & monitor costs, limit IT spend, scale to meet need, create cost accountability

Security baseline

Ensure compliance with IT security requirements by applying a security baseline to all adoption efforts



Resource consistency

Ensure consistency in resource configuration. Enforce practices for on-boarding, recovery, and discoverability

Identity baseline

Ensure the baseline for identity and access are enforced by consistently applying role definitions and assignments

Deployment acceleration

Accelerate deployment through centralization, consistency, and standardization across deployment templates

Governance funnels corporate policy changes into five actionable disciplines – **enabling your organization to modernize and reach business goals.**

https://aka.ms/adopt/Gov

Governance – develops and evolves corporate policies for:

- Resource consistency and management
- Security baseline
- Identity baseline
- Cost management
- Deployment acceleration

Cloud governance team
A team consisting of cloud architects, legal, security and/or HR & Finance develops and enforces these disciplines across your organization to ensure governance consistency.

veraqor
unveiling data, unleashing potential

Microsoft Azure

Governance as Actionable Model

veraqor
unveiling data. unleashing potential

Govern Methodology Disciplines

Cost Management

Govern

Business risks

Document evolving business risks and the business' tolerance for risk, based on data classification and application criticality

Define corporate policy

Policy and compliance

Convert risk decisions into policy statements to establish cloud adoption boundaries

Process

Establish processes to monitor violations and adherence to corporate policies.

Five disciplines of cloud governance

Cost management

Evaluate and monitor costs, limit IT spend, scale to meet need, create cost accountability

Security baseline

Ensure compliance with IT security requirements by applying a security baseline to all adoption efforts

Resource consistency

Ensure consistency in resource configuration. Enforce practices for on-boarding, recovery, and discoverability

Identity baseline

Ensure the baseline for identity and access are enforced by consistently applying role definitions and assignments

Deployment acceleration

Accelerate deployment through centralization, consistency, and standardization across deployment templates

veraqor

Cost Management

Establish controls and processes to ensure proper allocation of cost across business units, implement cost guardrails, and analyze the cost of applications.

Define

- Enterprise Enrollment Hierarchy Process and RACI Azure Cost Management Budgets and Alerts + RACI
- Cost Management RBAC Model

Define Cost Management Policies

- Tagging
- Allowed VM SKUs
- Allowed Storage SKUs
- Allowed Networking SKUs
- Allowed Database SKUs

Azure tools and services

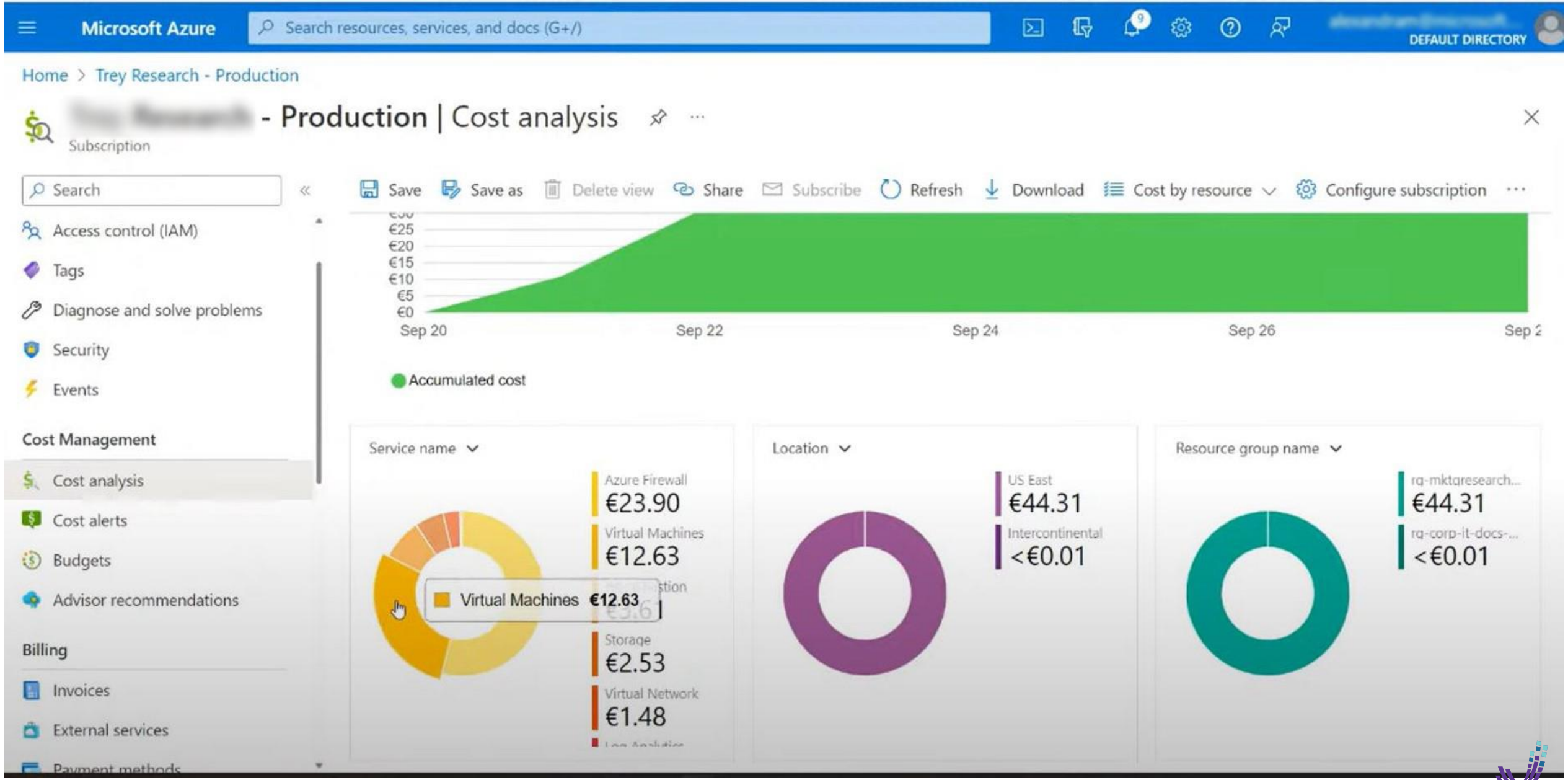
Azure Policy

Azure Cost Management PBI Application in Azure Marketplace

Azure Advisor

Azure Portal

Azure EA Content Pack


Microsoft Azure
Search resources, services, and docs (G+/)
DEFAULT DIRECTORY
Home > Trey Research - Production
- Production | Cost analysis
Subscription
Search
Access control (IAM)
Tags
Diagnose and solve problems
Security
Events
Cost Management
Cost analysis
Cost alerts
Budgets
Advisor recommendations
Billing
Invoices
External services
Payment methods
Save
Save as
Delete view
Share
Subscribe
Refresh
Download
Cost by resource
Configure subscription
€25
€20
€15
€10
€5
€0
Sep 20
Sep 22
Sep 24
Sep 26
Accumulated cost
Service name
Azure Firewall
€23.90
Virtual Machines
€12.63
Virtual Machines €12.63
Storage
€2.53
Virtual Network
€1.48
Location
US East
€44.31
Intercontinental
<€0.01
Resource group name
rg-mktgresearch...
€44.31
rg-corp-it-docs-...
<€0.01

Govern Methodology Disciplines

Security Baseline

Govern

Business risks

Document evolving business risks and the business' tolerance for risk, based on data classification and application criticality

Define corporate policy

Policy and compliance

Convert risk decisions into policy statements to establish cloud adoption boundaries

Process

Establish processes to monitor violations and adherence to corporate policies.

Five disciplines of cloud governance

Cost management

Evaluate and monitor costs, limit IT spend, scale to meet need, create cost accountability

Security baseline

Ensure compliance with IT security requirements by applying a security baseline to all adoption efforts

Resource consistency

Ensure consistency in resource configuration. Enforce practices for on-boarding, recovery, and discoverability

Identity baseline

Ensure the baseline for identity and access are enforced by consistently applying role definitions and assignments

Deployment acceleration

Accelerate deployment through centralization, consistency, and standardization across deployment templates

veraqor

Security Baseline

Establish policies to protect your network, assets, and data – residing on cloud provider platform(s).

Document risks, business tolerance, and mitigation strategies related to the security of:

- **Data and assets:** develop clear, simple, and well-communicated guidelines to identify, protect, and monitor the most important data assets
- **Network:** control and monitor any allowed communication between on-premises environment and cloud workloads.

Implement these best practices for corporate policy:

- **Network requirements:** on-premises networks must be secured against potential unauthorized access from cloud-based resources.
- **Hybrid identity strategies:** a key factor in structuring cloud-based identity services is the level of integration required with existing on-premises identity infrastructure.
- **Encryption:** encryption mechanisms vary in cost and complexity, and both technical and policy requirements and can influence decisions on how encryption is applied and how to store and manage critical secrets and keys
- **Security Baseline policies:** processes that manage updates to security policy based on inputs from stakeholders. (e.g., initial risk assessment and planning, deployment planning and testing, and quarterly review and planning)

Azure tools and services

Azure Policy

Azure Security Center

Azure Sentinel

Subscription Design

Encryption

Hybrid Identity

Azure Networking

Azure Automation

Sample Policies:
Security Baseline

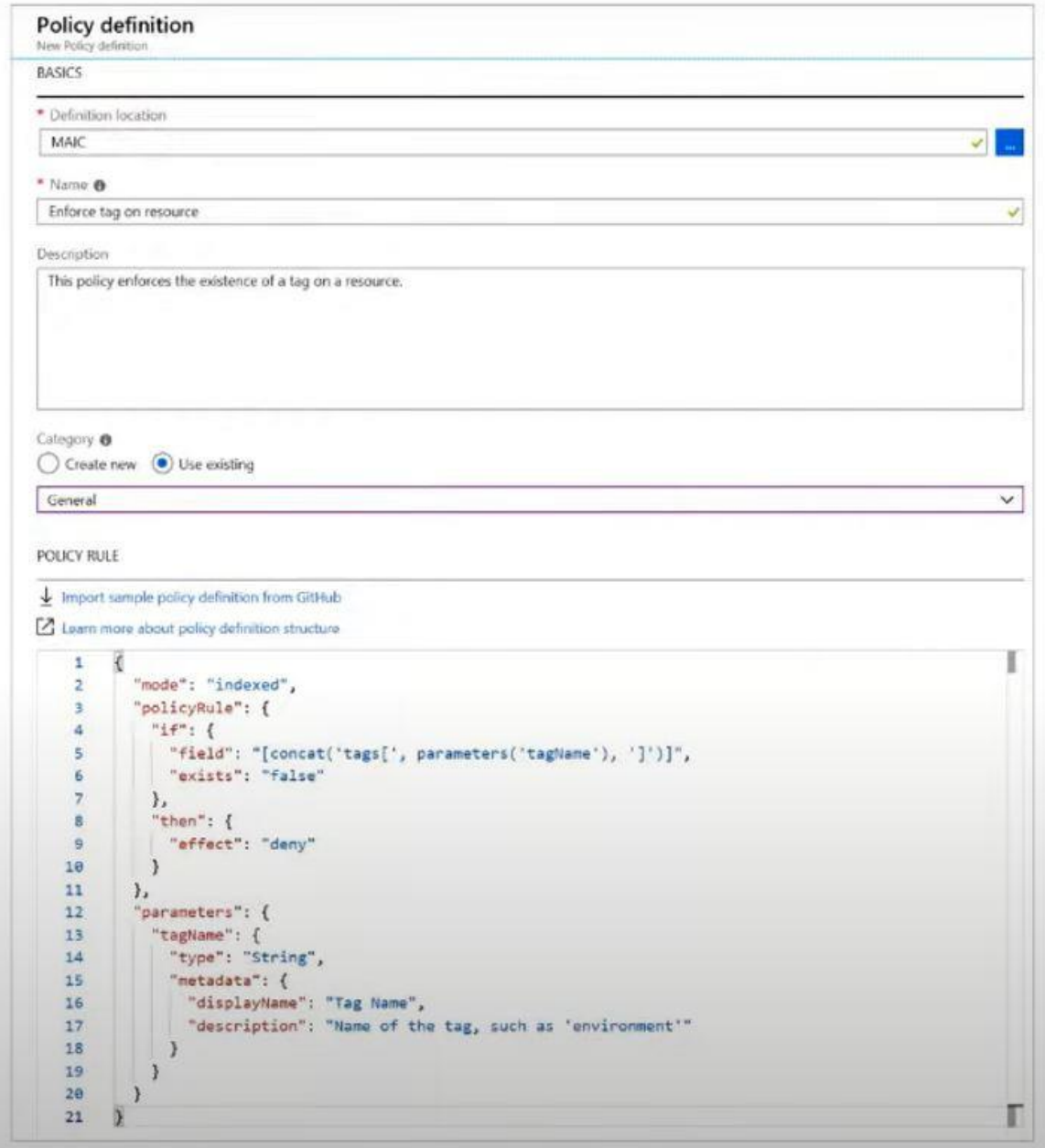
- All deployed assets must be categorized by criticality and data classification.
- All protected data must be encrypted when at rest.
- Network subnets containing protected data must be isolated from any other subnets. Network traffic between protected data subnets is to be audited regularly.
- All connections between the on-premises and cloud networks must take place either through a secure encrypted VPN connection or a dedicated private WAN link.
- No public facing web site backed by IaaS should be exposed to the internet without DDoS.
- Governance tooling must audit and enforce network configuration requirements defined by the Security Baseline team.
- Trends and potential exploits that could affect cloud deployments should be reviewed regularly by the security team to provide updates to Security Baseline tooling used in the cloud..

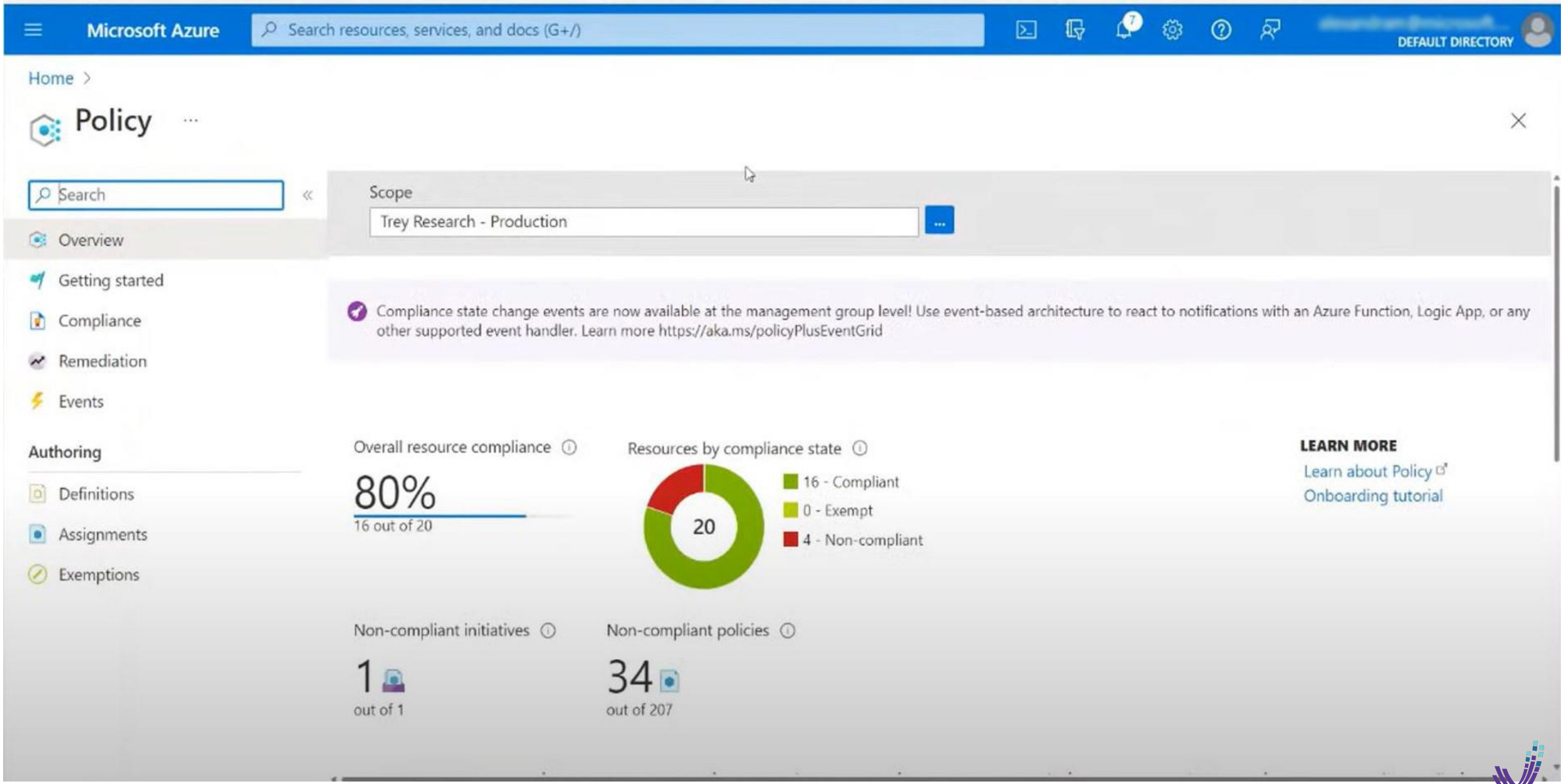
Azure Policy

These policies apply and enforce rules that your resources need to follow.

Examples:

- Only allow storage resources to be created
- Only allow resources in specific Azure regions
- Enforce the use of tag with every resource
- Enforce resource naming convention




Microsoft Azure
Search resources, services, and docs (G+/)
DEFAULT DIRECTORY
Home
Policy
Search
Overview
Getting started
Compliance
Remediation
Events
Authoring
Definitions
Assignments
Exemptions
Scope
Trey Research - Production
Compliance state change events are now available at the management group level! Use event-based architecture to react to notifications with an Azure Function, Logic App, or any other supported event handler. Learn more https://aka.ms/policyPlusEventGrid
Overall resource compliance
80%
16 out of 20
Resources by compliance state
20
16 - Compliant
0 - Exempt
4 - Non-compliant
LEARN MORE
Learn about Policy
Onboarding tutorial
Non-compliant initiatives
1
out of 1
Non-compliant policies
34
out of 207

Govern Methodology Disciplines

Resource Consistency

Govern

Business risks

Document evolving business risks and the business' tolerance for risk, based on data classification and application criticality

Define corporate policy

Policy and compliance

Convert risk decisions into policy statements to establish cloud adoption boundaries

Process

Establish processes to monitor violations and adherence to corporate policies.

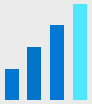
Five disciplines of cloud governance

Cost management

Evaluate and monitor costs, limit IT spend, scale to meet need, create cost accountability

Security baseline

Ensure compliance with IT security requirements by applying a security baseline to all adoption efforts



Resource consistency

Ensure consistency in resource configuration. Enforce practices for on-boarding, recovery, and discoverability

Identity baseline

Ensure the baseline for identity and access are enforced by consistently applying role definitions and assignments

Deployment acceleration

Accelerate deployment through centralization, consistency, and standardization across deployment templates

veraqor

Resource Consistency

Implement the foundation for governance best practices – with correct resource organization.

Define Azure Management Groups & Subscriptions model and RACI

- To reflect security, operations and business/accounting hierarchies
- To group similar resources into logical collections

Define resource consistency roles & responsibilities

- To further group applications or workloads into deployment and operations units

Define Resource Consistency Policies

- Naming Conventions
- Tagging
- Allowed Locations
- Allowed Resource Types
- Allowed Extensions
- Auditing

Azure tools and services

Azure Policy

Azure Monitor

Azure Advisor

Resource Manager Templates

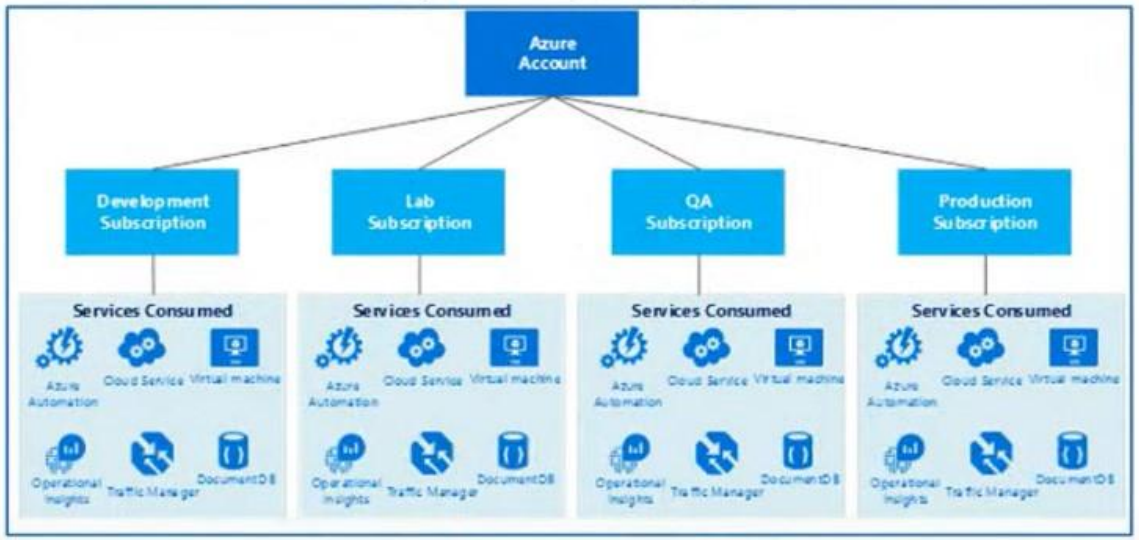
Resource Graph

Management Groups

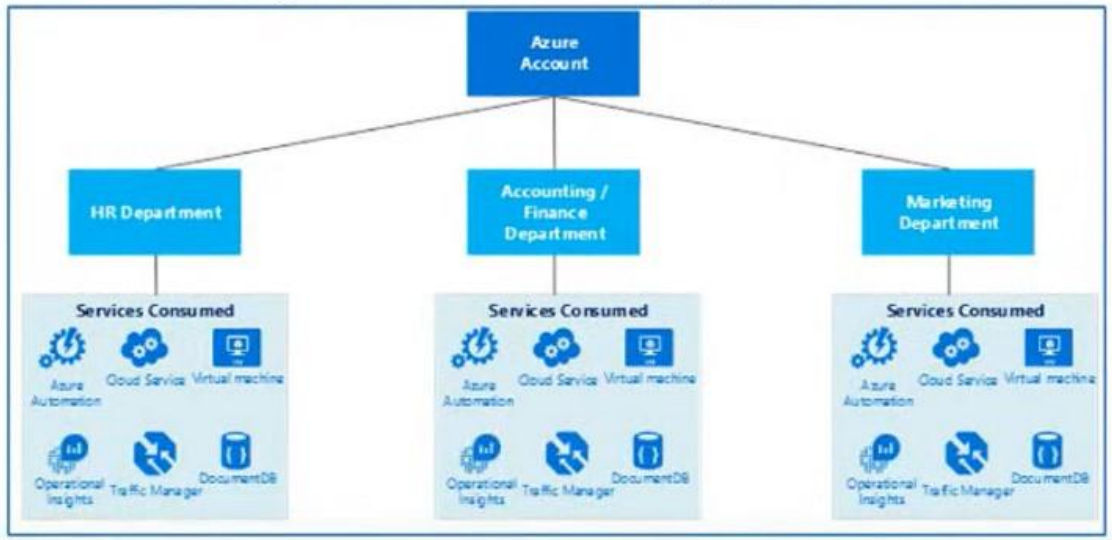
Subscription | Design considerations

Develop the Subscription, Network, Storage, Availability and Administrative models together in order to have a cohesive approach.

Service (Process) Design Model



Organizational Unit Design Model



Items to look at when designing the subscription model

Business Requirements
- Accountability
- Audit/Compliance
- Performance
- Availability & Recoverability

Technical Requirements
- Network Connectivity (shared or dedicated)
- Active directory requirements, clustering, identity, management tools

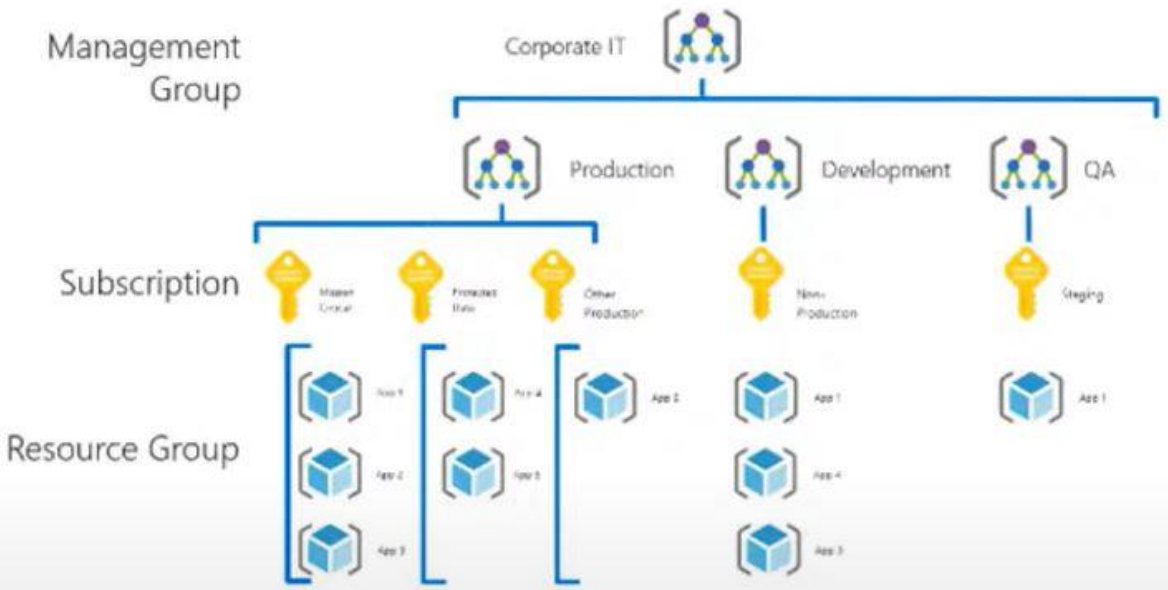
Security Requirements
- Who are the subscription administrators
- Least privilege model

Scalability Requirements
- Growth plans
- Allocation of limited resources
- Evolution over time (users, shared access, resource limits)

Microsoft Azure

Management Group best practices

- Define your hierarchy based on organization and environment type (prod, pre-prod, etc.)
- The root MG is for global configuration
  - Be careful with MG level assignments as they will cascade through large chunks of your hierarchy
- Try not to repeat yourself. Assign common policies and RBAC higher up in your hierarchy
- Built-in RBAC roles for MGs (MG contributor, MG reader)
  - Need subscription owner access to move to another MG



Implement a naming standard

Naming component	Description
Resource type	An abbreviation that represents the type of Azure resource or asset. This component is often used as a prefix or suffix in the name. For more information, see Recommended abbreviations for Azure resource types. Examples: `rg`, `vm`
Business unit	Top-level division of your company that owns the subscription or workload the resource belongs to. In smaller organizations, this component might represent a single corporate top-level organizational element. Examples: `fin`, `mktg`, `product`, `it`, `corp`
Application or service name	Name of the application, workload, or service that the resource is a part of. Examples: `navigator`, `emissions`, `sharepoint`, `hadoop`
Subscription purpose	Summary description of the purpose of the subscription that contains the resource. Often broken down by environment or specific workloads. Examples: `prod`, `shared`, `client`
Environment	The stage of the development lifecycle for the workload that the resource supports. Examples: `prod`, `dev`, `qa`, `stage`, `test`
Region	The Azure region where the resource is deployed. Examples: `westus`, `eastus2`, `westeu`, `usva`, `ustx`

Example:

- Virtual Network

  vnet-<subscription purpose>-<region>-<###>

  - `vnet-shared-eastus2-001`
  - `vnet-prod-westus-001`
  - `vnet-client-eastus2-001`

To simplify this process, we recommend using the Azure Naming Tool. Find it at aka.ms/AzureNamingTool

Govern Methodology Disciplines

Identity Baseline

Govern

Business risks

Document evolving business risks and the business' tolerance for risk, based on data classification and application criticality

Define corporate policy

Policy and compliance

Convert risk decisions into policy statements to establish cloud adoption boundaries

Process

Establish processes to monitor violations and adherence to corporate policies.

Five disciplines of cloud governance

Cost management

Evaluate and monitor costs, limit IT spend, scale to meet need, create cost accountability

Security baseline

Ensure compliance with IT security requirements by applying a security baseline to all adoption efforts

Resource consistency

Ensure consistency in resource configuration. Enforce practices for on-boarding, recovery, and discoverability

Identity baseline

Ensure the baseline for identity and access are enforced by consistently applying role definitions and assignments

Deployment acceleration

Accelerate deployment through centralization, consistency, and standardization across deployment templates

veraqor

Identity Baseline

Protect your data and assets in the cloud – implementing identity management and access control.

Define Azure RBAC Model

- Using RBAC can segregate duties within a team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in an Azure subscription or resources, only certain actions with narrow scope can be allowed.

Define Azure Access Management Process and RACI

- Several options are available for managing identity in a cloud environment which vary in cost and complexity.
- A key factor in structuring your cloud-based identity services is the level of integration required with existing on-premises identity infrastructure.

Operationalize Azure Privileged Identity Management

- Cloud-based identity management is an iterative process.

Azure tools and services

RBAC

Azure AD

Azure AD B2B

Azure AD B2C

Directory Federation

Directory Replication

Azure Role-Based Access Control (RBAC)

- Fine-grained access control to Azure "control plane"
- Grant access by assigning Security Principal a Role at a Scope
  - Security Principal: User, group, or service principal
  - Role: Built-in or custom role
  - Scope: Subscription, resource group, or resource
- Assignments are inherited down the resource hierarchy

Learn more https://aka.ms/azureiam

Govern Methodology Disciplines

Deployment Acceleration

Govern

Define corporate policy

Business risks

Document evolving business risks and the business' tolerance for risk, based on data classification and application criticality

Policy and compliance

Convert risk decisions into policy statements to establish cloud adoption boundaries

Process

Establish processes to monitor violations and adherence to corporate policies.

Five disciplines of cloud governance

Cost management

Evaluate and monitor costs, limit IT spend, scale to meet need, create cost accountability

Security baseline

Ensure compliance with IT security requirements by applying a security baseline to all adoption efforts

Resource consistency

Ensure consistency in resource configuration. Enforce practices for on-boarding, recovery, and discoverability

Identity baseline

Ensure the baseline for identity and access are enforced by consistently applying role definitions and assignments

Deployment acceleration

Accelerate deployment through centralization, consistency, and standardization across deployment templates

veraqor

Deployment Acceleration

Establish policies to govern asset configurations or deployments – manual, or automated through DevOps best practices.

The DevOps practices in this discipline include:

Infrastructure as code

- Stand up environments in the fastest means possible.
- Remove the human element and reliably and repeatable deploy every time.
- Improve environment visibility and improve developer efficiency
- Store infrastructure definitions alongside application code.

Continuous integration and continuous deployment

- Accelerate delivery through automation
- Simple and easy to use
- Global community for actions

Azure services that enable deployment acceleration include Azure Blueprints

Deploy and update cloud environments in a repeatable manner using composable artifacts

Azure tools and services

Resource Manager Templates

Azure PowerShell

Azure CLI

Azure Policy

Resource Grouping & Tagging

Azure DevOps

Github – Azure Github Actions

Azure Automation

Microsoft Azure

Define Your Initial Governance State – Leverage the Governance Benchmark Assessment

veraqor
unveiling data. unleashing potential

Drive cloud adoption efficiency in an iterative governance process – four key exercises to focus on:

1 **Methodology overview**
Establish a basic understanding of cloud governance

2 **Governance benchmark**
Assess your current state and the future state to get started

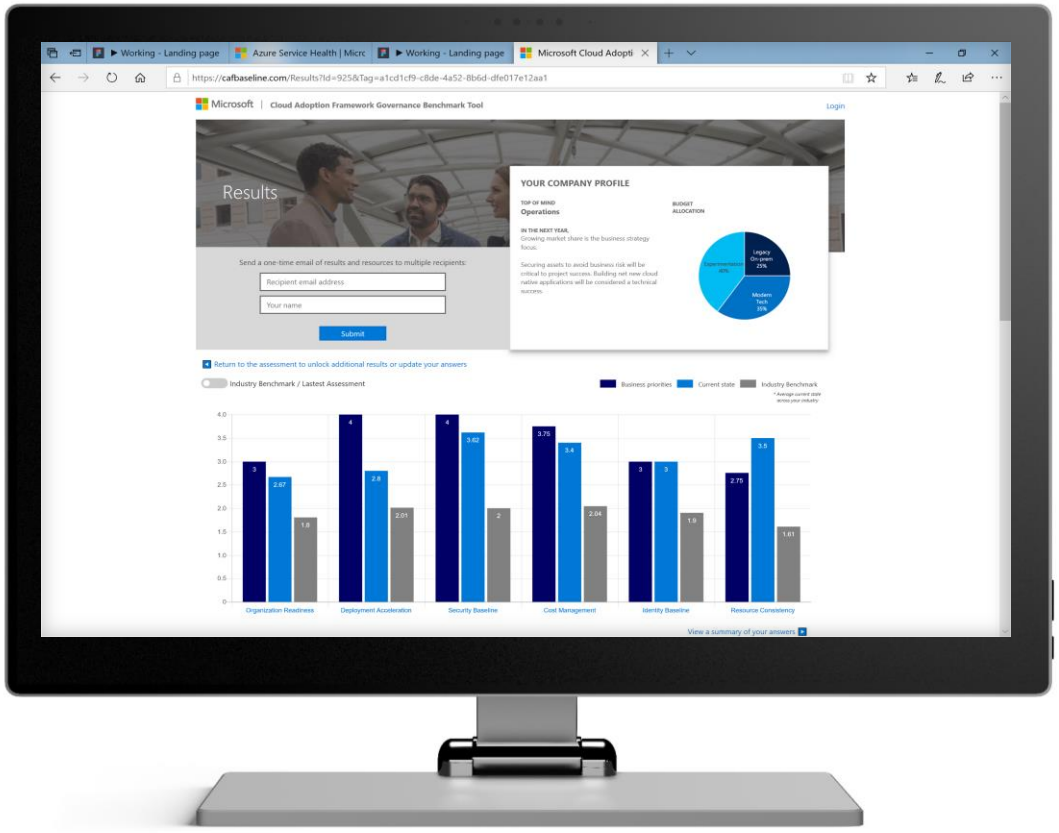
3 **Initial governance foundation**
Begin establishing your governance foundation by implementing a set of governance tools

4 **Evolve governance foundation**
Iteratively add governance controls to address risks

Benchmark Your Governance State

Make governance **actionable** with **processes and policies.** Use the Governance benchmark tool.

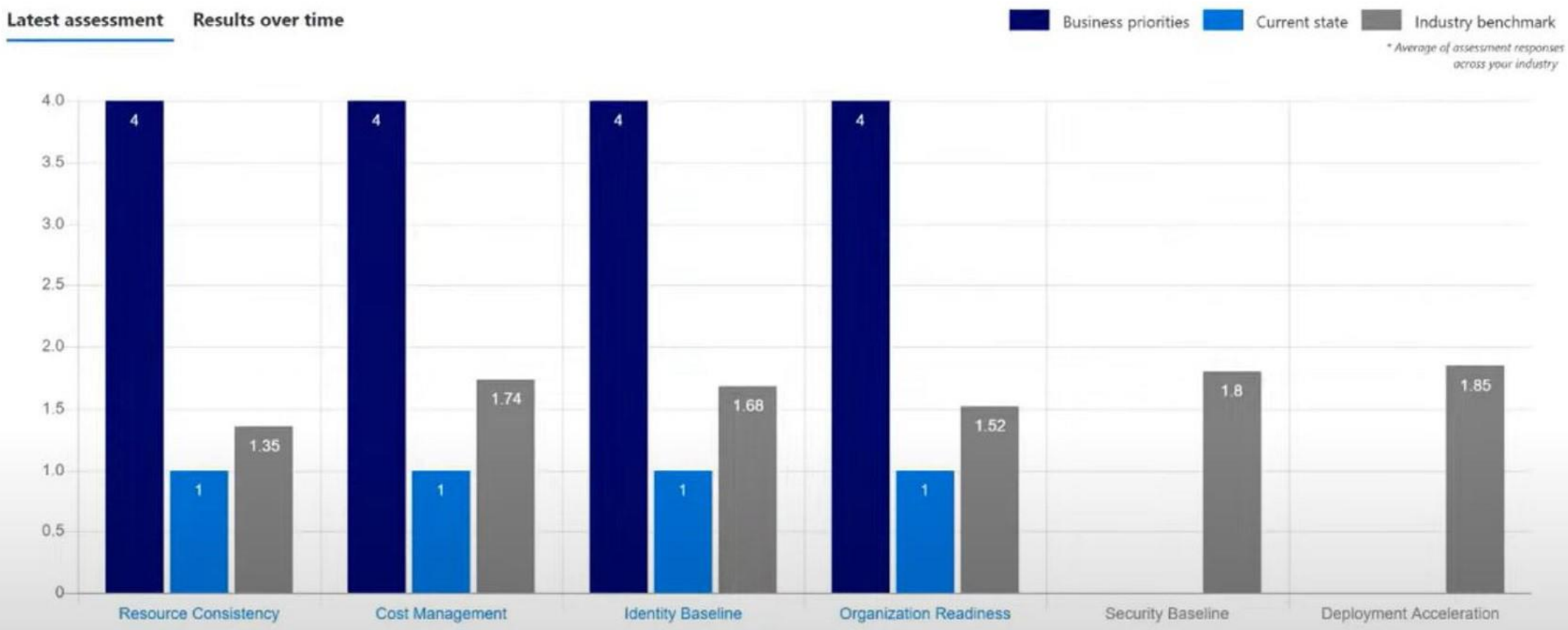
- Establish a governance baseline **and recommended starting-point**
- Understand gaps **between your desired and current governance state, using the Cloud Adoption Framework**.
- Remove blockers **with curated guidance on how to build a proper Governance foundation**.



https://cafbaseline.com/

veraqor

Benchmark Assessment Results



* Domains in the graph are sorted by the highest gap between business priorities and current state

View a summary of your answers ▶

veraqor

Microsoft Azure

Take action and set up your initial governance foundation

veraqor
unveiling data. unleashing potential

Drive cloud adoption efficiency in an iterative governance process – four key exercises to focus on:

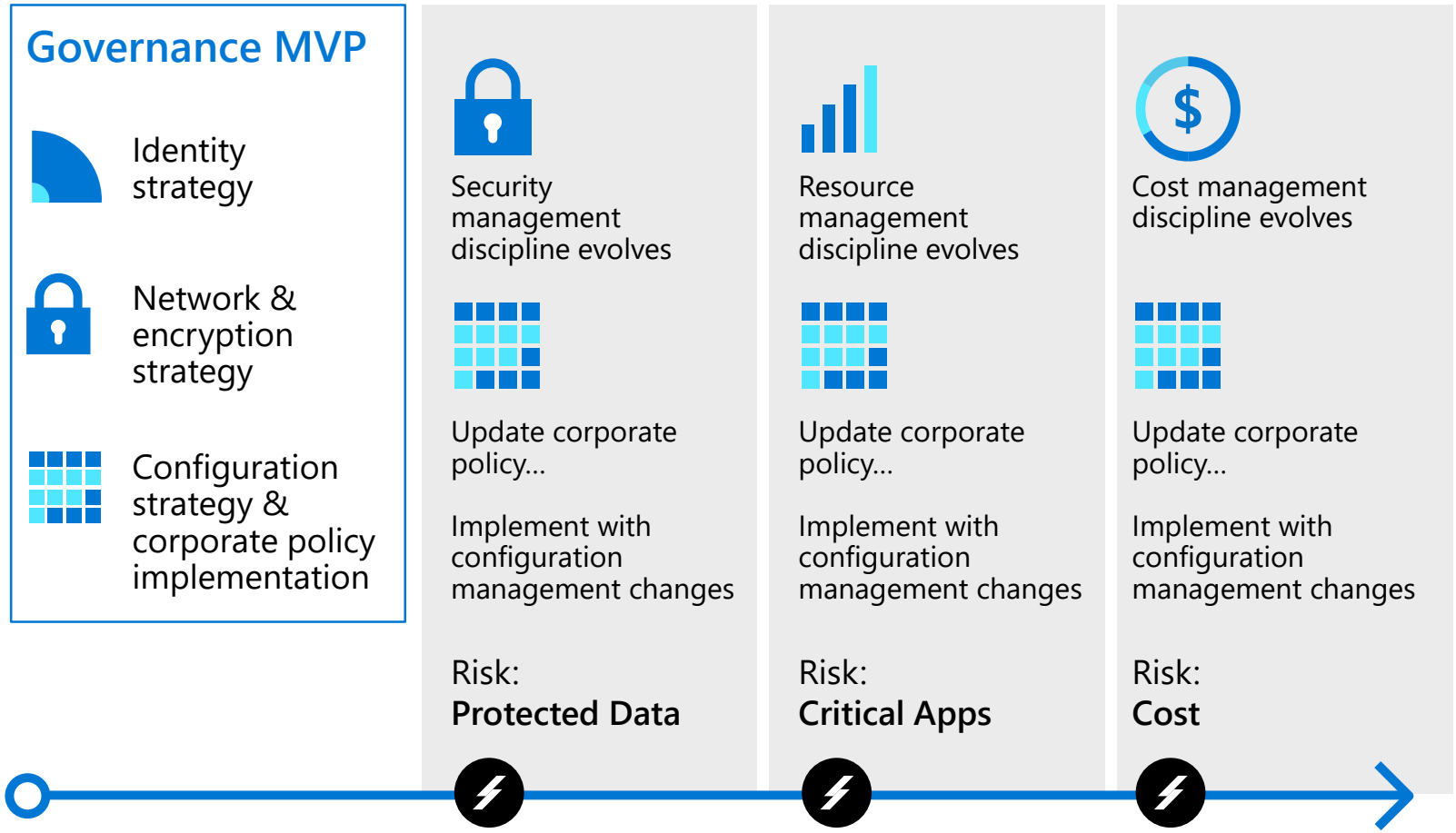
1 **Methodology overview**
Establish a basic understanding of cloud governance

2 **Governance benchmark**
Assess your current state and the future state to get started

3 **Initial governance foundation**
Begin establishing your governance foundation by implementing a set of governance tools

4 **Evolve governance foundation**
Iteratively add governance controls to address risks

Executing Incremental Governance



Adoption timeline will trigger **risks** along the journey

Governance MVP

Establish a foundation that can quickly evolve as cloud adoption and cloud governance mature. Mitigate tangible risks identified in the cloud adoption plan.

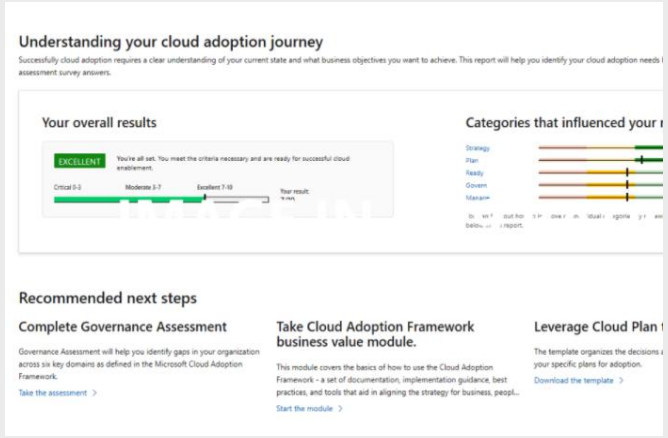
Risk Evolutions

The risk profile will change as you plan additional iterations of cloud adoption. The cloud governance team monitors those adoption plans to identify risks and evolve corporate policy statements.

Build the Governance MVP

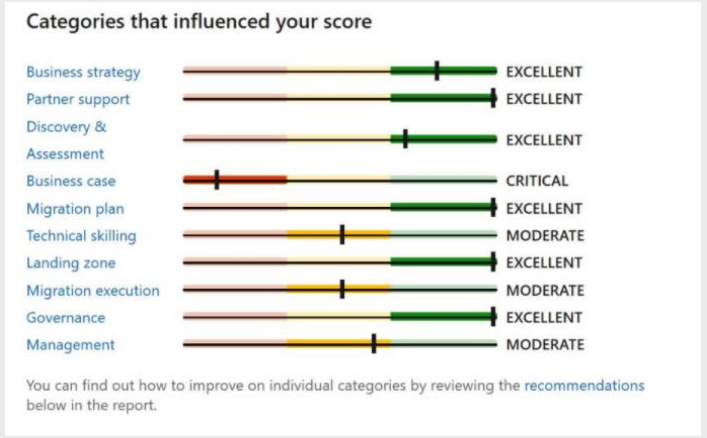
Standard Enterprise	Complex Enterprise
1. Customers or staff reside largely in one geography	1. Customers or staff reside in multiple geographies or require sovereign clouds
2. Business units share a common IT infrastructure	2. Customers or staff reside in multiple geographies or require sovereign clouds
3. Single IT budget	3. Budget allocated across business units and currencies
4. Capital expense-driven investments are planned yearly and usually cover only basic maintenance	4. Capital expense-driven investments are planned yearly; often include maintenance and refresh cycles of 3-5 years
5. Datacenter or third-party hosting providers with fewer than five datacenters	5. Datacenter or third-party hosting providers with more than five datacenters
6. Networking includes no WAN; or 1-2 WAN providers	6. Networking includes complex network or global WAN
7. Identity is a single forest, single domain	7. Identity consists of multiple forests, multiple domains
8. Cost Management (cloud accounting) showback model – billing is centralized through IT	8. Cost Management (cloud accounting) chargeback model – billing can be distributed through IT procurement
9. Security Baseline – protected data: company financial data and IP. Limited customer data. No third-party compliance requirements.	9. Security Baseline (protected data) – Multiple collections of customers' financial and personal data

Evaluate Your Cloud Readiness using Microsoft Assessments



Cloud Journey Tracker

Identify your cloud adoption needs and find recommendations for your unique cloud journey.



Strategic Migration Assessment & Readiness Tool

Understand your organization's preparedness to implement a cloud migration at scale.

Governance Benchmark

Identify gaps in your organization's current state of governance and get curated guidance on how to get started.

veraqor

How Can Veraqor Help?

Briefing	Assessment	Proof of Concept	Implementation
Understand the Importance and key benefits of Azure Governance & Compliance	**Governance Architecture** will be shared after assessment of subscription.	**POC provides** a test bed where we can migrate your workloads and applications to a cloud environment	**Governance Architecture** Subscription will be migrated to governance architecture.
Briefly discuss about Implementation Of Azure Governance and Its Disciplines including Cost Management, Security Baseline, Resource Consistency, Identity Baseline, Deployment Acceleration	**Assessment Report** will be shared on 5 key areas of Microsoft Azure Governance	**Azure high level design**, Analysis and Planning report, Pre-Engagement Questionnaire	**Documentation** around the governance mapping, architecture, and migration roadmap.
Training and Best Practice regarding Azure Governance tools	**Migration Plan** will be shared including ARM template and onboarding through Azure lighthouse	**It makes your business** more efficient and saves time and money	**Training and best practices** regarding Azure Governance tools
Duration: 2 Hours Investment: **FREE**	Duration: 3 Weeks Investment: **$10,000**	Duration: 3 Weeks Investment: **$6,000**	Duration: 6 Weeks Investment: **$25,000**

veraqor

Microsoft Azure

Thank you!

Please spare a moment to fill out the survey after this webinar.

Need help? Please write to:

mtu@veraqor.io

veraqor
unveiling data. unleashing potential